Philip Kiko
Chief Administrative Officer

Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515-6860

February 3, 2017

To: The Honorable Gregg Harper
Chairman, Committee on House Administration

The Honorable Robert A. Brady
Ranking Member, Committee on House Administration

From: Philip G. Kiko
Chief Administrative Officer

Paul D. Irving
Sergeant at Arms

Subject: Revoking IT and Physical Access for Identified Shared Employees

Timeframe: Urgent

Summary

The House Inspector General (OIG) and HIR Cybersecurity have documented multiple procurement irregularities, IT security violations, and shared employee policy violations by five shared staff employed by multiple House offices, hereafter referred to as "the employees". Based upon the evidence gathered to this point, we have concluded that the employees are an ongoing and serious risk to the House of Representatives, possibly threatening the integrity of our information systems and thereby Member's capacity to serve constituents.

The employees are:

1. Rao Abbas
2. Hina Alvi
3. Imran Awan
4. Jamal Awan
5. Abid "Omar" Awan

Given the scope of the documented activity and the ongoing risk to Members and the House, we request that the Committee authorize the Chief Administrative Officer (CAO) and the Sergeant at Arms (SAA) to revoke the access of the employees to all House IT systems and non-public facilities.

We are very appreciative of the complete and total support we have received from the Member offices we have cooperated with during this review. Impacted offices have been cooperative and

responsive to the needs of the inquiry and their full support has greatly informed this recommendation.

With the approval of the Committee, the CAO and the SAA will take the following actions:

- Disable and remove all access to House information technology resources, including both network and local accounts.
- Disable and remove access to email accounts, remote access accounts/tokens, mobile phones and devices.
- Disable any prox card access.
- Demand that these individuals surrender equipment.
- Revoke all parking passes and privileges.
- Instruct all House office Members' and their staff where these employees worked to change their House account passwords and personal passwords (e.g., iTunes) that they may have shared with these employees.
- Request that the House Superintendent rekey any room or facility used by the employees to store data or equipment.
- In an effort to protect Member's inventory, alert the United States Capitol Police to be on alert for any suspicious activity related to House assets and property by the employees.

Background

- In March of 2016, the CAO Office of Acquisitions Management discovered suspicious purchase orders for mobile equipment by Mr. Omar Awan[1], a shared employee of multiple Member offices. Mr. Awan structured these purchase orders in such a way as to bring the asset price below the accountable equipment threshold of $500.[2]
- The Chief Administrative Officer reported the suspicious activity to the Committee on House Administration. The Committee on House Administration requested the OIG to initiate a formal inquiry of this activity.
- After reviewing the initial purchase orders, vouchers, and emails, the OIG's inquiry widened to include the above referenced individuals. While performing the inquiry, the OIG discovered evidence of irregular procurements as well as violations of both IT security and shared employee policies. We have determined twenty House offices were victims of the procurement irregularities, and potentially over 40 House Offices may have been victims of IT security violations.
- In September of 2016, as the size and scope of the inquiry widened, the Committee on House Administration and the OIG briefed the former Chairman of the Democratic Caucus about suspicious activity related to their server that the OIG identified. As a result, the former Chairman of the Democratic Caucus directed the CAO to copy the data from their server and two computers.

---

[1] Not to be confused with a CAO employee of the same name.

[2] The individual requested that the equipment vendor reduce the asset purchase price to below $500 and inflate the cost of the extended warranty to compensate.

- The Committee on House Administration directed the Inspector General to refer the matter to the United States Capitol Police (USCP). The USCP initiated an investigation that continues to this day.
- In late 2016, the former Chairman of the Democratic Caucus announced his intention to resign from Congress to assume a new position. The CAO and SAA worked with the Chairman to account for his inventory, including the one server.
- While reviewing the inventory, the CAO discovered that the serial number of the server did not match that of the one imaged in September. The CAO also discovered that the server in question was still operating under the employee's control, contrary to the explicit instructions of the former Chairman to turn over all equipment, and fully cooperate with the inquiry and investigation.
- The USCP interviewed relevant staff regarding the missing server.
- On January 24, 2017, the CAO acquired the server from the control of the employees and transferred that server to the USCP.

Summary of Evidence Gathered by the House OIG

Prior to turning over the inquiry to the USCP, the OIG gathered significant evidence related to the procurement irregularities and IT security policy violations by the employees. The evidence packet assembled by the OIG has been provided to you.

The packet includes:

1. Spreadsheet of House vouchers documenting irregular transactions;
2. Spreadsheet from CDWG documenting open balances;
3. Purchase orders and vouchers documenting structured purchases;
4. Interview notes with House Member's Chiefs of Staff;
5. Interview notes with equipment vendor;
6. Equipment inventories and forms;
7. Job history and wages of each employee;
8. Logon activity and computer access logs;
9. Pictures of boxes of stored equipment; and,
10. OIG analysis documents.

The following summarizes the findings of the OIG; supported by the evidence packet.

Summary of Procurement Irregularities

The *Guide to Outfitting and Maintaining an Office for the U.S. House of Representatives* issued by the Committee on House Administration requires the CAO to maintain an inventory of all Member and Committee office equipment items having an original purchase price of $500 or more. The OIG documented numerous instances of the employees structuring purchases and comingling assets to avoid controls over property and equipment.

The OIG documented:

- Thirty-four purchases totaling nearly $38,000 where the employees structured the purchase to avoid the $500 accountable equipment threshold, without the Member's knowledge.
- $219,000 in outstanding invoices owed to CDW-G for purchases orchestrated by these employees, some of which were for invoices more than 500 days old, all of which are unknown to the Member's office.
- Eighty-three pieces of missing equipment with a purchase price of $118,683.80 that had been "written off" from the House inventory by CAO staff at the direction of the shared employees. Missing equipment included laptops, iPads, TVs, video conferencing equipment, and computers.
- Fourteen examples of equipment delivered to the home of some of the employees, instead of the House of Representatives, thus bypassing internal controls during the receiving process.
- Examples of unopened equipment being stored at unknown locations for long periods.

Summary of Shared Employee Regulation Violations

The House Ethics Manual, 2 U.S.C. § 4701, and Committee on House Administration *Shared Employee Manual* all prohibit the sharing or subletting of job duties with other individuals employed by 1) different Member or Committee offices or 2) individuals who are not on the House payroll.

The CAO has documented that in both calendar years 2015 and 2016, each employee acknowledged that he or she had read and understood the *Shared Employee Manual*. Specifically, the employees acknowledged that they would:

- The pay I receive from each employing authority will reflect the duties actually performed for each employing authority.
- I will inform each employing authority, in writing, of all of the offices for which I am working, and will inform each employing authority, in writing, or any change in this status.
- I will neither share my job duties nor sublet any portion of my official duties.
- I will utilize House assigned email accounts for all of my work for House offices.
- I will have an established system to keep all House records under my control secure.
- I am currently, and will take all necessary steps to remain, in compliance with the mandatory provisions of law and regulation described in the *Shared Employee Manual*, and will abide by all House statutes, rules and regulations, whether they are or are not noted in this certification or the Shared Employee Manual.

The OIG documented:

- The five employees shared job duties with one another even though different offices employed them.
- Numerous examples of the employees intermingling computer equipment with the offices they supported, without the knowledge of their employing offices. The summation of the OIG's interview with one Chief of Staff is of note:

> Coming in on a Saturday and finding Omar in the office with equipment everywhere. She stated, "It looked like Christmas with little TVs, iPods, etc. scattered around the room." She stated that Omar told her "these items were not

her office's equipment but they belonged to another office." She told him to get them out of her Member's office.

- One Member office believed the employees were contractors, not House employees. Furthermore, the office believed that one of the employees ran the enterprise as a business, with the other four employees effectively reporting to him.
- One of the employees appears to have violated outside fiduciary restrictions on senior staff.

Summary of House IT Security Policy Violations

The OIG documented numerous and egregious violations of House IT Security, including:

- *Principles of Behavior for Information System Users:* Users must access and use only information for which they have official authorization.
- *HISPOL 002.0 Protecting Systems from Unauthorized Use Section 2.2* - Users shall access and use only information for which they have official authorization.
- *HISPOL 009.00 Password Protection: Policy 2.6* – Do not share UserIDs and passwords with anyone.
- *HISPOL 010.0* – Protection of Sensitive Information, Section 2.3 – All House sensitive information must be stored on House owned equipment.
- *HISPOL 016.00 Security Policy for Privileged Account Management* - Security Section 3.3.7 - Multiple users shall not share access to an individual Privileged Account.

Examples of such violations documented by the OIG include:

- These employees accessed user accounts and computers for offices that did not employ them, without the knowledge or permission of the impacted Member's office.
- The employees established permissions in offices so that each of the five could administer computers in other offices. This could have resulted in Member's data being accessed by someone unknown and unauthorized by the office. HIR Cybersecurity identified 107 workstations supported by the shared system administrators that have groups outside of the workstation's office assigned administrative permissions.
- One of the employees accessed accounts, including some assigned to Members, nine times in September 2016. The offices who owned these accounts did not employ the employee. These accesses occurred on Democratic Caucus computers, even though the employee had never been employed by the Democratic Caucus, and without the knowledge of the Democratic Caucus.
- Four of the employees accessed the Democratic Caucus computers 5735 times, even though the Democratic Caucus did not employ these employees. HIR Cybersecurity speculates that the employees used the Democratic Caucus server as an entry point and jumping off point to access computers for other House offices.
- Forty logons to computers the employees were not authorized to access.
- The sharing of passwords and accounts by the employees, including sharing privileged accounts.
- The unauthorized storage of sensitive House information outside the House.